SECURITY DOCUMENTATION

LAM-FOR KWOK, PEGGY P K FUNG AND DENNIS LONGLEY

cslfkwok@cityu.edu. hk *peggy@cs.cityu.edu.hk* *peggy@cs.cityu.edu.hk*
City University of Hong Kong
Department of Computer Science
83 Tat Chee Avenue
Kowloon
Hong Kong
Tel : (852) 27888625 (852) 27844234 (852) 27889723
Fax: (852) 27888614

Keywords: Security standards, security documentation, risk analysis, countermeasures, security model.

Abstract: Information Security Management Standards and Code of Practice provide guidance on good practice for security officers. However there is still a significant gap between the security officer's real world environment and the advice provided by information security professionals and consultants.

This paper suggests that a uniform approach to security documentation may provide a first step in bridging that gap, and discusses a proposed structure for such documentation. It is clear from this discussion, however, that a first attempt at security documentation reveals a more fundamental problem, the lack of a working security model. Having documented the local security scenario, the security officer requires some means to extract security relevant information, e.g. to advise management on the current state of organizational security and to recommend security priorities. This paper concludes with a discussion on such a security model.

1. INTRODUCTION

The advent of BS7799, which has been adopted by countries like AS 4444 in Australia and has been accepted as an ISO 17799 standard, was hailed as a major advance in security management, but having given seminars on Information Security Management Standards to security officers, one gains the impression that the gap between theory and practice is still very wide.

In fact one is sometimes left with the suspicion that the Standards may have done more to solve the problems of security audit and training organizations, than those of the security officer. Of course, the security officer can take out insurance and persuade management to fund a compliance audit. The results of such an audit will enable the security officer to either:

- Display a certificate on the wall, or
- Present management with a list of resources necessary to acquire such a certificate.

But then what? How does the security officer set about ensuring that the organization, which will probably have an ever increasing business dependency on its expanding and vulnerable I.T. system, is as well protected as limited security resources allow?

A security incident could cause serious financial losses to an organization, its partners and clients. In these litigious days the security officer could well face a hostile barrister, in the aftermath of such a security incident. It is not difficult to predict the type of questions that would be asked; formulating convincing responses might be more problematic. How can security officers demonstrate that they take all reasonable efforts, to optimally deploy security resources?

Accountants have long since recognized that their professional competence may be demonstrated by a pristine set of financial records. An accountant will probably give a high priority to the maintenance of such records, when accepting a new appointment. Hence accountancy students are taught bookkeeping in their first year, however, few information security courses and textbooks provide an insight in the development and maintenance of information security documentation.

It is suggested that a comprehensive set of security documentation can serve to guide the security officer to an optimal information security stance, and to provide convincing evidence that a reasonable standard of professional competence had been maintained.

Security documentation can, inter alias:

- Document all significant policies pertinent to information security;
- Provide details of all systems and environments for which the officer has security responsibilities;
- Specify the security officer's responsibilities as formulated by senior management;
- Specify the degree to which some of those responsibilities have been delegated;
- Document the security systems and procedures developed in response to those responsibilities;
- Provide clear pointers to security logs and records, and reporting/ archiving responsibilities;
- Record the outcomes and subsequent actions, following risk analysis and security audits;
- Facilitate the design of security systems for new and enhanced IT systems;
- Facilitate audit and compliance exercises; and
- Provide senior management with an overview of the organization's security stance.

It is therefore suggested that the security officer should give careful consideration to the development and continual maintenance of an appropriate set of security documentation. Having said that leads to the obvious follow up question - how?

The standards such as BS7799 group together security topics, and implicitly encourage a top down approach to security management, but they do not explicitly advise the security manager on the development of security documentation. Indeed, one of the significant dangers of the standards is that they will encourage the formation of security documentation, which serves to facilitate compliance audits, but does little to enhance organizational I.T. security.

In this paper the role of security documentation is discussed and some suggestions are provided on the development of electronic documentation to facilitate information security management.

2. TOTAL SET OF SECURITY DOCUMENTATION

2.1 Overview

The potential applications of information security documentation were listed above and this list provides an insight into the proposed set of documentation. Since we are dealing with information security in a complex and dynamic I.T. environment, the documentation should clearly be maintained in electronic form, with databases employed for all items comprising significant amounts of detail, and html linkages between relevant sections.

The proposed sections of the security documentation are:

- Policies,
- Information Assets,
- Systems and Environments,
- Responsibilities,
- Security Systems and Procedures,
- Records, Reporting and Archiving,
- Security Audits and Business Continuity Planning,
- System Development, and
- Compliance.

The various proposed sections are described in outline below.

2.2 Policies

Organizational security policies commonly come in one of three varieties - the *non-existent,* the *bland* and the *treatise* on *passwords.* The security officer is well advised to explore and document all the implicit and explicit organizational policies, which could have some impact upon information security. These policies may then be used to establish the various aspects of the organization's information security policy.

Organizations will have, at least implicit, policies to ensure their continued existence, by abiding with all legislative, regulatory and contractual requirements. Such requirements commonly have implications for the integrity, availability and often confidentiality, of certain records and hence on security requirements.

The assets and finances of an organization are subject to control and recording policies: authorizations, four eyes principles, segregation of duties, audit trails etc. As such manual processes migrate to I.T. systems, these policies also remain as significant security requirements.

Some policy areas may have more subtle impacts upon information security. The deleterious effects of offensive email, in a climate increasing sensitivity to harassment and discrimination issues, were easily predicted. Nevertheless some organizations still lack systems and procedures to respond to such misuse of information systems. Similarly social concerns may lead to demands for accessibility to certain organizational information, or for dial up access for classes of disadvantaged employees, with attendant network security implications.

The part of Privacy Policy that related to the protection of personal data will clearly have implications to information security. The current and emerging laws on intellectual property will also be a major concern, particularly in terms of installed software and material downloaded from the Web.

Personnel policies, and related outsourcing issues, will have less subtle impacts upon information security, particularly if they produce a high level of mobility amongst privileged information system users, or contract out I.T. processing without strict contractual requirements on information security.

The information security officer would thus be well advised to hold documentation on all relevant management policies, to consider them and to report upon their implications for the organizational security policy.

2.3 Information Assets

The security officer is responsible for the protection of the information assets, but what are these assets and what degrees of priority are given to them? The problem of assigning dollar values to electronic files was recognized in the days of Courtney Risk Analysis [1], and the current problem is much more complex than that. The questions faced by the security officer are, inter alias, *what is the business impact arising from the*:

- Loss of confidentiality of this data item
- Loss of integrity of this data item;
- Unauthorized invocation of this transaction; and
- Loss of availability of this business process for this specified period of time.

Even the development of an inventory of the total set of data assets is a task ranging from the mammoth to the impossible. Nevertheless the security

officer should at least document classes of data and business processes, together with a mapping to the systems storing, processing and transmitting those classes, and if possible an impact rating of the classes. Given the draconian laws arising on intellectual property the security officer will need to maintain a register of all installed software and license agreements.

2.4 Systems and Environments

It is self evident that the security officer should document the relevant details of all lT systems, buildings etc. within their aegis. The problem is to ensure that this documentation is continually updated in current networked environments. Ideally the I.T. departments would supply this information electronically, and security officers then merely require a linkage from this documentation. In such a case, is there some mechanism by which the security officer can highlight recent actual or proposed changes so that the security implications can be considered?

At the other end of the spectrum, the production and maintenance of this aspect of the documentation may be extremely time consuming. Such a situation is one requiring urgent attention, since it implies that the security officers are not adequately informed of the systems and environments they are required to protect.

2.5 Responsibilities

No security system is 100% effective and security officers commonly complain of a lack of support from senior management. In these circumstances security officers cannot guarantee that security incidents never arise, and they will implicitly bear some degree of responsibility for any consequent business impacts. Hence the security officers would be wise to obtain a full statement of their own responsibilities, and develop an organizational chart showing the explicit delegation of those responsibilities.

The security officer should also be in a position to call upon a full description of the security responsibilities of all employees, contractors etc. In the event of a security incident this documentation should be able to highlight either:

- The individuals that failed to meet their security responsibilities, or
- Inadequate, or unrealistic, specification of security responsibilities.

Delegation of security responsibilities also implies a commitment to ensure that such delegations are not unreasonable in terms of the expectations placed upon employees. Hence this set of documentation should also contain full details of the proposed and actual systems for

security training, with links to training material, course details, staff attendances etc.

2.6 Security Systems and Procedures

The documentation must clearly contain details of security systems, e.g. firewalls, VPNs, swipe card access control, virus protection software, authentication servers etc. and associated procedures, e.g. allocation of access privileges and passwords, Much of this material is commonly embedded in other documentation and, in the first instance, a comprehensive set of linkages should be established.

The security officer clearly needs to have access to such details of security systems and procedures in the first instance. However, this section of the documentation also provides an insight into the role of the security officer, because it raises a number of significant questions:

- How do these security systems and procedures correlate with the *systems and environments* documentation (See 2.4)?
- What are the role of these security systems and procedures, i.e. what assets are they protecting against what threats?
- What are the threats and assets that are not covered by these systems and procedures?
- Are the strongest security systems and procedures directed to the highest areas of risk?
- What is the degree of effectiveness of the systems and procedures - prioritised in order of risk?
- Do any of these systems and procedures represent, in themselves, single points of failure?
- Are these systems and procedures themselves vulnerable to attack?

Clearly these questions cannot be answered by an inventory of security systems and procedures. Such a discussion involves the complex linkages between all the entities involved a risk analysis: threats, systems (physical and logical), vulnerabilities, security systems, information assets and the organizational reliance upon those assets. The security officer requires an effective active security model to tackle these questions (See 3). A security officer would do well to reflect that the questions posed above could well be asked by a hostile barrister, in legal case following security incident that caused financial loss to other parties.

2.7 Records, Reporting and Archiving

Senior management, legal and law enforcement advice is essential, to develop a full understanding of the security officer's responsibilities in protecting and/or maintaining:

- Organizational reports and archives as required by senior management policy, regulatory or legislative bodies; and
- Operating and security logs and reports.

This section of the security documentation should contain details of those sets of data, e.g. tax return information, essential to ensure organizational compliance with contractual, legal, regulatory or legislative requirements.

Linkages or cross references to other sections of the security documentation are also recommended e.g.

- Systems and environments (See 2.4): where are the records stored and processed?
- Responsibilities (See 2.5): who are responsible for their security?
- Security systems and procedures (See 2.6): what are the security provisions for their protection?
- Security audits (See 2.8): were any recommendations made for their protection and what subsequent action was taken?

The operating and security logs and reports are clearly of vital importance. This set of documentation should be headed by all relevant advice, from legal and law enforcement agencies, on the collection, handling and retention of such data, particularly in respect of data that may be used in legal proceedings.

In addition to the security reports and logs themselves, this section must contain all relevant supporting documentation to ensure that the reports and logs can at some later date be filly exploited in investigations and, if necessary, submitted in legal proceedings. Linkages and cross references to other documentation will include, inter alias:

- Systems and environments (See 2.4) to ensure that details as of the date that the records were taken are available; and
- Responsibilities (See 2.5) particularly in relation to capturing security data.

2.8 Security Audits and Business Continuity Planning

A comprehensive set of security documentation will greatly facilitate security audits, and security audit reports etc. can themselves be a valuable

component of security documentation. Such reports will normally provide an overview of the security situation at the time of the audit and a series of recommendations.

The security officer should document not only the reports but also the follow up actions to the recommendations; including a follow- up schedule, showing the progress of implementation and also reasons for delayed or non-implementation. There is ample material available on the documentation of Business Continuity Planning and it is suggested that such documentation may also be maintained in this section, with appropriate linkages to the other sections.

2.9 System Development

In many cases security officers have responsibility for protecting systems that were not designed with a high priority given to security. Hence it is important that a security officer provides well-documented and reasoned cases for security implementation in new or upgraded systems. In the cases of system modification or upgrade the security officer needs to give careful consideration to:

- The risks of the current system;
- The security, and security rationale, provided against those risks;
- The risks of the proposed system;
- Proposed removal of any erstwhile security systems or procedures; and
- The security and security rationale to be provided against the risks of the proposed system.

If the risks, security and security rationale of the erstwhile system were adequately documented then this exercise is greatly facilitated. If such documentation is not available then there is a significant danger that system changes will introduce new risks, or remove undocumented, but important, security systems or procedures of the original system. The discussion in a proposed security model (See 3) is relevant to this section.

2.10 Compliance

This section of the documentation should provide an overview of the security stance of the organization and highlight any major areas of concern by cross linkages, e.g. management policies that are not being met by current security systems and practices, security audit recommendations still outstanding, inadequate security logging in case of a security incident etc.

In this section the security officer would be wise to make a detailed list of security recommendations for senior management, and record them for that interview with the hostile barrister.

3. SECURITY MODEL

3.1 Overview

One of the major problems with most security documentation is that it is commonly embedded in documentation intended for another purpose, e.g. Operating Manuals, System Design Reports etc. Documentation intended primarily for security purposes tends to be addressed at a macro level, e.g. standards, risk analysis report. Information at this level tends to focus on *what security is to be achieved* rather than how *to achieve it*. Rarely does one read current documentation and feel that it gives a genuine insight into the security stance of an organizational system, i.e. it is often difficult to answer the major questions of the security officer: where do I need to focus attention, what are the priorities for the future.

The Risk Data Repository (RDR) [24] was developed some years ago as a risk analysis model, and during this work it became clear that the RDR also provided an insight into the requirements for security documentation. A prototype system was developed in Visual Basic and current work is directed to developments, which could make more effective use of PC browsers to handle the linkages amongst the entities. It also clear that the early RDR did not adequately address the role of networks.

Nevertheless the RDR described entities in terms of their roles from a security viewpoint, demonstrated the security inter-relationships of those entities and facilitated the computation of risk parameters. The entities of the earlier model are being replaced with a greater emphasis on networks and countermeasures. It is suggested that this model provides a basis for security documentation in electronic form that can:

- Be easily updated in rapidly evolving environments; and
- Facilitate the extraction of security information for various purposes, e.g. risk analysis, security design etc.

3.2 Structure of Security Entities

In the discussion on documentation above it was suggested that the security officer maintain documentation on *Information Assets*, Systems and

Environments, Security Systems and Procedures and System Development. It was also noted that it would normally be quite difficult to extract the information required by the security officer from current documentation.

It is suggested that a security model could provide a means by which a security officer records the relevant security information and gradually builds up application packages to assist in the analysis of that information. In the first instance the entities of the model are defined, followed by the security linkages for such entities. The proposed entities relate the physical and logical aspects of security. At the top end of the model the *Information Assets* are processed by *Application Systems,* which in turn are hosted by *Virtual Networks.* These *Virtual Networks* are in turn hosted by *Physical Networks.* The *Physical Networks* comprise a set of interconnected *Units,* and are located in *Physical Platforms,* which themselves are located in a *Physical Environment.*

The purpose of the model is to highlight the security inter-relationships between the entities in a manner that facilitates the task of the security officer. The major entities included in the model are:

- A Unit - individual item of equipment + plus its accessories. Unit come in four categories End User (EU), Server (SU), Sensitive Data Storage Unit (SDSU) and Coms (CU) (NB cabling and wireless is considered as a Coms Unit).
- A PHYSICAL NETWORK (PN) - a collection of interconnected Units, one or more of which is a cabling or wireless Unit.
- A PHYSICAL PLATFORM (PP) - a collection of standalone Units and all SDSUs and physical networks located in a physical area.
- A PHYSICAL ENVIRONMENT - a collection of sites and buildings with associated essential services and physical security funnctions that hosts Physical Platforms.
- A VIRTUAL NETWORK (VN) - one or more physical networks, with common security architecture and / or a grouping associated with an AS.
- AN APPLICATION SYSTEM (AS) - one or more virtual networks used to host an information processing and/or communication application.
- INFORMATION ASSETS (IA) - data and processes, which, if attacked, could cause significant harm to the organization.
- INTRINSIC THREATS (IT) - those events that may cause harm to information assets and whose occurrence cannot be prevented, e.g. environmental threats (fire, extreme weather conditions), personnel physical (damage or misuse of equipment) and personnel logical (attacks mounted over networks etc).

These entities have, however, been chosen so that the linkages between them provide security officers with an insight into the security of their systems. These linkages are described in the next section.

3.3 Inter-relationships of Security Entities

The security entities described in the previous section are inter-related from a security viewpoint. The emphasis is now on the physical network, as the logical grouping of equipment items. If a building (Physical Environment) hosting a Physical Platform is damaged by some intrinsic threat event, e.g. fire, the security officer will be more interested in the effect upon a Physical Network than an individual item of equipment. Any standalone items will be separately linked to the Physical Platform and to the Application System. The security entities facilitate the tracing of threat events to their ultimate consequence, which is a business impact. If the model is recorded as an electronic document, with html links, then the security officer can easily postulate a number of potential intrinsic threats and then trace their likely paths to determine the ultimate business impact. The threats may be classified as:

- Environmental (e.g. flooding): impacting upon Physical Environments,
- Personnel Physical (e.g. attacker enters secure area containing an SDSU): impacting upon Physical Platforms, and
- Personnel Logical (e.g. attacker gaining access to sensitive server over a network): impacting upon Virtual Networks.

Having traced an attack the security officer will then be concerned with the degree to which the security measures mitigate such an attack. In this model it is suggested that such security measures can be effectively represented as Threat Countermeasure Diagrams [5]. In this approach each countermeasure is considered to counter the incident threat but also to introduce consequent threats arising from loopholes in the countermeasure or attacks on the countermeasure itself. Supporting countermeasures are commonly employed to address these consequent threats, and a Threat Countermeasure Diagram is an effective means of representing such countermeasure rationale.

4. CONCLUSIONS

The life of an airline pilot is sometimes described as hours of boredom followed by minutes of sheer terror. The life of a security officer could

similarly be described as years of frustration, followed by weeks of severe recrimination. Effective security documentation can be a means by which security officers can:

- Gain an enhanced awareness of their roles and the procedures to fulfil those roles;
- Provide evidence to senior management on necessary security systems and procedures; and
- Provide evidence on their professional competence.

It has also been suggested in this paper that such documentation could be significantly enhanced by an electronic security based similar to the Risk Data Repository described in previous papers.

5. REFERENCES

[1] Courtney, R.H. JR., "Security risk assessment in electronic data processing systems." *AFIPS Conference Proceedings* 1977, pp.97-104.

[2] Anderson, A.M., Longley, D., and Tickle, A.B., "The Risk Data Repository: A Novel Approach to Security Risk Modelling". *Computer Security, Proc. IFIP TC 11 9th Int. Conf. on Information Security* (Editor Dougall), IFIP Sec.'93, Toronto, Canada, 12-14 May 1993, NY:Elsevier Science Publishers, 1993, 185-190.

[3] Anderson A, Kwok L F and Longley D, "Security Modelling for Organisations", *Proc. of 2nd ACM Conf on Computer and Communication Security,* Fairfax Virginia, USA, 2-4 Nov 1994, pp.241-250.

[4] Kwok L F and Longley D, "A Security Officers' Workbench", *Computers and Security,* Vol.15, No. 8, 1996, 695-705.

[5] Caelli, W., Longley, D., and Tickle, A.B. "A Methodology for Describing Information and Physical Security Architectures". *IT Security: The Need for International Cooperation, Proc. IFIP TC11 8th Int. Conf. on Information Security* (Editors Gable and Caelli), IFIP Sec.'92, Singapore, 27-29 May 1992, NY:Elsevier Science Publishers, 1992, 277-296.